REMARKS

I. Claim Objections

The Examiner suggested that the term "a Certificate verifier component" in claim 16, line 29 be amended to "a certificate verifier component." Applicant as amended claim 16 as suggested.

The Examiner objected to "said each server" in claim 10, line 3 as lacking antecedent basis. Applicant respectfully traverses. Claim 7 recites "transferring to each server of said server systems. . . ."

The Examiner objected to "said different fingerprints" in claim 14, line 1 as lacking antecedent basis, and suggested it be amended to "said two different fingerprints." Applicant has amended claim 14 as suggested.

The Examiner objected to "said common data store" in claim 16, line 36 as lacking antecedent basis. Applicant has amended this claim to recite "said common data base," thereby obviating this objection.

The Examiner objected to "the computer" in claim 17, line 4 as lacking antecedent basis. Applicant has amended an earlier reference to "a digital computer," thereby obviating this objection.

II. Rejections under Section 112

The Examiner rejected claims 1, 4, 5, 7, 8, and 9 under 35 U.S.C. 112, second paragraph, because it was unclear whether "third tier server certificates," "third tier certificate," "original third tier certificate," and "received third tier certificate" refer to the same element. Applicant has amended these claims to recite "server-copy" and "client-copy" of the third tier server certificate, as appropriate. Applicant notes, however, that despite its use of the term 'copy,' the exact information transmitted to each entity may vary somewhat.

The Examiner rejected claims 1, 2, 4, and 5 under 35 U.S.C. 112, second paragraph, because it was unclear whether "all necessary information," "necessary information," and "information" refer to the same component. Applicant has replaced all three formulations with "at least all necessary information."

The Examiner rejected claims 7, 12, and 16 under 35 U.S.C. 112, second paragraph, because it was unclear whether "third tier server," "third tier server system," and "server system" refer to the same element. Applicant has amended these claims to recite "application server systems" and "third tier server systems," as appropriate.

III. Rejections under Section 101

The Examiner rejected claims 12-16 under 35 USC 101 because the server and client components have not been limited to hardware in the Specification. Applicant acknowledges that the inventions in claims 12-16 can be implemented in hardware, software, or a combination thereof. However, Applicant respectfully asserts that the claims, as amended, the standards articulated in the recent Federal Circuit *Bilski* decision. Claim 12 is now directed to a specific machine, namely an application server in a distributed application environment, comprising:

> a transfer server component which, in a first computer process, supports non-continuous and secure client-server connection for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system,
>
> a connection negotiator component which, in a second computer process receives incoming third tier server certificates via a secure connection between said application server systems and said third tier server, and
>
> a certificate verifier component which, in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from said client.

Claim 16 is similarly directed to a specific machine, namely a client system for authenticating third tier server in a distributed application environment comprising:

> a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server,
>
> a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment,
>
> a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common data base if it matches, and
>
> a user interface component which, in a fourth computer process, allows for accepting or rejecting an unknown third tier server certificate not contained in said common data base,

a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmits them to said application server systems via a secure connection.

IV. Rejections under section 103

The Examiner rejected claims 1, 4-9, and 16-17 under 35 U.S.C. 103(a) as being unpatentable over Patent Publication 2002/0152382 ("Xiao") in view of Applicant's Background Section. The Examiner also rejected claims 2-3 and 10-15 under Section 103(a) as unpatentable over Xiao, Applicant's Background Section, and U.S. Patent No. 6,233,577 ("Ramasubramani"). Applicant respectfully traverses.

A. Claim 1

The invention in claim 1 is generally directed at a method for authenticating a third tier server system in a distributed application environment, said distributed application environment comprising client system having parts of the distributed application, server systems having the remaining parts of the distributed application. As noted in Applicant's specification at paragraph [0025], a "significant difference to the prior art is that no database for the certificates at the server side is needed anymore." Applicant's specification goes on to state that a major enhancement compared to the prior art is that "[n]o local certificate database exists on the server systems. Certificate verification is processed exclusively by means of the certificate information sent by the client system. There is no need to administer any third tier certificates locally on the server systems." *Id. At ¶ [0049] (element numbers removed)*

Xiao, in contrast, is directed at a delivery scheme that allows clients to verify received certificates in a two-tier client-server system. In this system, the server sends its server certificate to the client. *Xiao at ¶ [0074].* The client then hashes the server certificate, and then compares the result hash with a list of trusted entity 'thumbprints' stored in a 'trusted information object.' *Id. at ¶ ¶ [0074]-[0076].* Xiao also describes updating the trusted information object HTTP, or broadcast. *Id. at ¶ ¶ [0081]-[0090].* Because Xiao is directed at a two-tier system, however, Applicant respectfully asserts that Xiao fails to teach or suggest a system where "at said server systems side said method comprises receiving from said common database of said client system

at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server" and "comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system."

Applicant's Background section also fails to teach or suggest these elements. In fact, Applicant's background section identifies as a drawback that "Each server application has a local certificate database which means additional effort to maintain and to protect the certificate data."

Ramasubramani also fails to teach or suggest these elements. Instead, Ramasubramani is also merely directed to a two-tier system where the client and server can send each other their certificates.

B. Claims 7, 12, and 16

Claims 7, 12, and 16 contain limitations similar to those discussed with respect to claim 1. Therefore, for the reasons discussed above, Applicant respectfully submits that the proposed combinations also fail to teach or suggest these claim limitations.

C. Claims 2-6, 8-11, 13-15, and 17

These claims are dependent on claims 1, 7, 12, or 16. Accordingly, the proposed combinations also fail to teach or suggest all elements of these claims.

V. Miscellaneous Amendments

To better protect the invention in the marketplace, Applicant has replaced "all necessary information" with the broader term "at least all necessary information" or the broader term "certificate information." Applicant has also replaced the transition "consists" in claims 4-6 with the broader transition "consist essentially of." In addition, Applicant has replaced "extracting" in claim 16 with "generating" to cover both certificate information extracted from the communication from the third tier server and certificate information calculated by the client. These amendments will affect the scope of these claims.

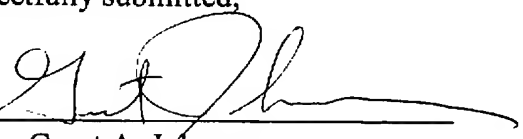
Applicant has added new claims 18 and 19 containing language from the original preamble test of claims 12 and 16, respectfully.

Applicant also made numerous amendments to correct grammar errors and/or to improve clarity.

VI. Conclusion

In view of the above amendments and remarks, Applicant submits that this Application is in condition for allowance and respectfully request reconsideration and withdrawal of the rejections and objections. The Examiner is urged to call the undersigned at the below-listed telephone number if, in the Examiner's opinion, such a phone conference would expedite or aid in the prosecution of this Application.

Respectfully submitted,

By: 

Grant A. Johnson
Registration No. 42,696

Telephone: (507) 253-4660
Fax No.: (507) 253-2382